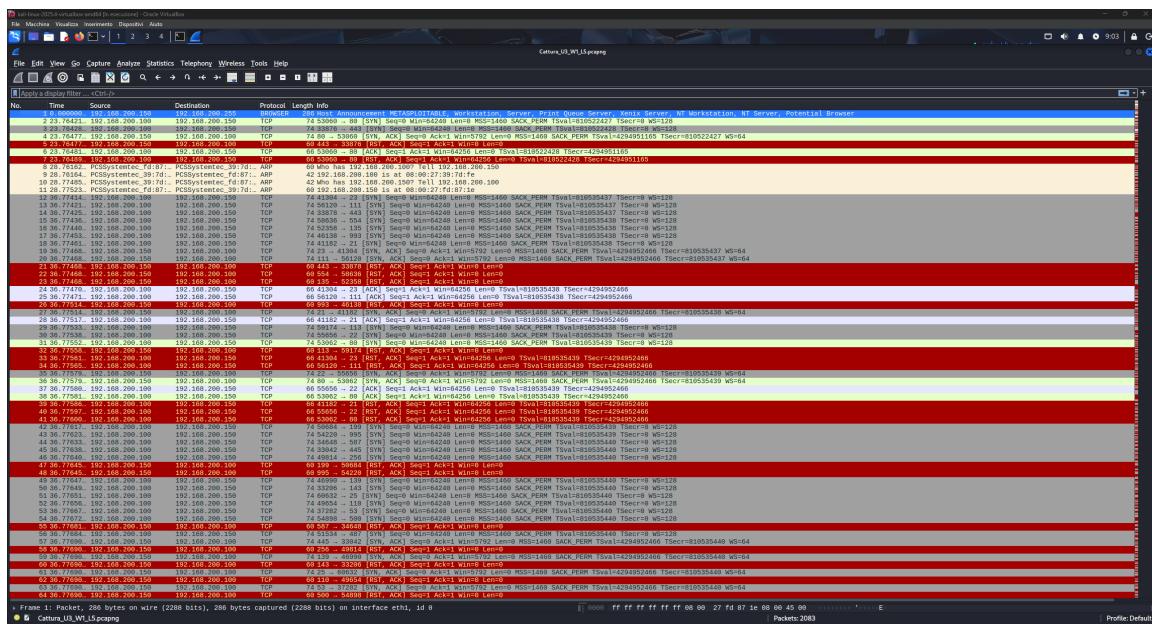


Report Tecnico: Network Traffic Analysis

Forensic Analysis of TCP Port Scanning Activity

Studente: Josh Van Edward D Abanico

Data: 6 febbraio 2026



Oggetto: Analisi Forense - Port Scanning Detection
Tool Utilizzato: Wireshark

Indice

1	Introduzione e Scenario Operativo	2
1.1	Obiettivi dell'Analisi	2
1.2	Topologia della Rete Ricostruita	2
2	Fase 1: Analisi Cronologica dell'Attacco	2
2.1	Annuncio Spontaneo della Vittima	2
2.2	Verifica Attività (TCP Ping)	2
2.3	Network Discovery (ARP)	3
2.4	Attacco alle "Top Ports" (Initial Burst)	3
2.5	Enumerazione Infrastruttura e Mail (Second Wave)	4
2.6	Chiusura Sessioni e Noise Scanning	5
2.7	Rilevamento Servizi Legacy Critici (Porta 512)	5
2.8	Conferma Vulnerabilità R-Services (Porta 514)	6
2.9	Identificazione R-Login (Porta 513)	6
3	Fase 2: Approfondimento Tecnico (Stealth vs Connect)	8
3.1	Differenze Teoriche: TCP Connect vs SYN Stealth	8
3.2	Analisi Forense	8
3.3	Deduzione Investigativa	8
4	Fase 3: Risultati dell'Enumerazione	10
4.1	Criticità Massima: Suite "R-Services" (Legacy)	10
4.2	File Sharing e Infrastruttura	10
4.3	Accesso Remoto e Web	10
5	Conclusioni	11

1 Introduzione e Scenario Operativo

1.1 Obiettivi dell'Analisi

Il presente documento riporta l'analisi tecnica di una cattura di traffico di rete (PCAP). L'obiettivo primario è caratterizzare la tipologia di traffico anomalo rilevato tra due host della rete locale, identificare le tecniche di riconoscimento utilizzate dall'attaccante e mappare la superficie di attacco esposta dalla vittima.

1.2 Topologia della Rete Ricostruita

Dall'analisi dei pacchetti ARP (Address Resolution Protocol) e del traffico TCP, è stata definita la seguente topologia:

- **Attaccante (Scanner):** 192.168.200.100
- **Vittima (Target):** 192.168.200.150
- **Asset Inventory:** Il target è identificato come una macchina virtuale "Metasploitable 2", progettata intenzionalmente con vulnerabilità per scopi di testing (banner rilevato nel pacchetto n. 1).

2 Fase 1: Analisi Cronologica dell'Attacco

2.1 Annuncio Spontaneo della Vittima

Al pacchetto n. 1 (Time 0.000), la macchina vittima invia un messaggio broadcast **NetBIOS Host Announcement**, rivelando spontaneamente la propria presenza e il proprio nome host ("METASPLOITABLE") all'intera rete, senza alcuna sollecitazione esterna.

2.2 Verifica Attività (TCP Ping)

Circa 5 secondi prima della scansione principale (pacchetti 2-7), l'attaccante esegue un controllo di disponibilità ("Host Discovery") per verificare se il target è attivo. Vengono inviati pacchetti **SYN** mirati verso le porte standard 80 (**HTTP**) e 443 (**HTTPS**).

- La ricezione di un [SYN, ACK] dalla porta 80 (pacchetto 4) conferma all'attaccante che l'host è acceso e raggiungibile.
- L'attaccante chiude immediatamente la connessione preliminare con un **RST** (pacchetto 7), avendo ottenuto la conferma necessaria per procedere con l'attacco massivo.

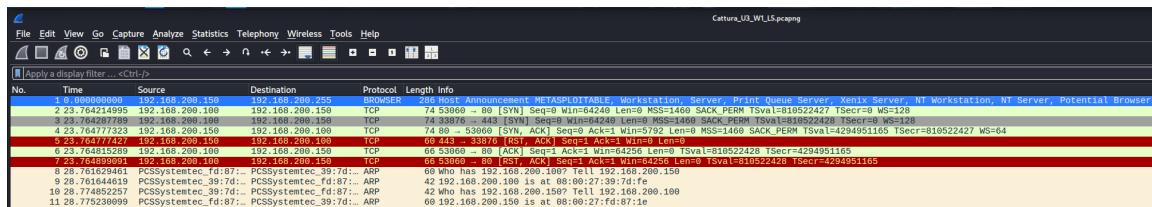


Figura 1: Pre-Attacco: Host Announcement spontaneo e TCP Ping di verifica (Porte 80/443).

2.3 Network Discovery (ARP)

L'attività ostile inizia con una fase di discovery locale. L'host attaccante esegue richieste ARP broadcast ("Who has 192.168.200.150?") per risolvere l'indirizzo fisico (MAC Address) della vittima, preludio necessario a qualsiasi comunicazione IP diretta.

8 28.761629461 PCSSystemtec_fd:87... PCSSystemtec_39:7d... ARP 60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619 PCSSystemtec_39:7d... PCSSystemtec_fd:87... ARP 42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257 PCSSystemtec_39:7d... PCSSystemtec_fd:87... ARP 42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230999 PCSSystemtec_fd:87... PCSSystemtec_39:7d... ARP 60 192.168.200.150 is at 08:00:27:fd:87:1e

Figura 2: Richieste ARP broadcast.

2.4 Attacco alle "Top Ports" (Initial Burst)

Immediatamente dopo aver ottenuto il MAC Address della vittima (pacchetto 11), l'attaccante lancia una raffica simultanea di richieste [SYN] verso le porte TCP più comuni ("Top Ports"), visibile dai pacchetti 12 al 18. Questa fase è mirata a identificare rapidamente i servizi standard prima di procedere con una scansione completa.

L'analisi dei pacchetti di risposta (dal 19 al 41) permette di delineare immediatamente il profilo di sicurezza della vittima:

- Servizi Aperti (Open):** La vittima risponde [SYN, ACK] sulle porte **21 (FTP)**, **23 (Telnet)**, **80 (HTTP)**, **111 (RPC)** e **22 (SSH)**.
- Servizi Chiusi (Closed):** La vittima invia un [RST, ACK] per le porte cifrate o più moderne come **443 (HTTPS)** e **993 (IMAPS)**.

- Riga 12:** Attaccante invia SYN.
- Riga 19:** Vittima risponde SYN, ACK.
- Riga 24:** Attaccante invia ACK (Connessione stabilita).
- Riga 33:** Attaccante chiude con RST, ACK.

12 36 .774143446	192.168.200.100	192.168.200.150	TCP	74 41394 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535437 Tscr=0 WS=128
13 36 .77422110	192.168.200.100	192.168.200.150	TCP	74 56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535437 Tscr=0 WS=128
14 36 .7743657841	192.168.200.100	192.168.200.150	TCP	74 56120 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535437 Tscr=0 WS=128
15 36 .7743636985	192.168.200.100	192.168.200.150	TCP	74 59360 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=0 WS=128
16 36 .774405627	192.168.200.100	192.168.200.150	TCP	74 52358 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=0 WS=128
17 36 .774535534	192.168.200.100	192.168.200.150	TCP	74 46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=0 WS=128
18 36 .774685776	192.168.200.100	192.168.200.150	TCP	74 51182 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=0 WS=128
19 36 .774685900	192.168.200.100	192.168.200.150	TCP	74 41394 - 4184 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=0 WS=128
20 36 .774685952	192.168.200.100	192.168.200.150	TCP	74 111 - 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM Tsva=4294952466 Tscr=810535437 WS=64
21 36 .774685690	192.168.200.150	192.168.200.100	TCP	68 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36 .774685737	192.168.200.150	192.168.200.100	TCP	68 554 - 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36 .774685776	192.168.200.150	192.168.200.100	TCP	68 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36 .774711972	192.168.200.150	192.168.200.100	TCP	68 41394 - 4184 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=4294952466
25 36 .774711972	192.168.200.150	192.168.200.100	TCP	68 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535438 Tscr=4294952466
26 36 .775141184	192.168.200.150	192.168.200.100	TCP	68 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 36 .775141273	192.168.200.150	192.168.200.100	TCP	74 21 - 41184 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM Tsva=4294952466 Tscr=810535438 WS=64
28 36 .775174048	192.168.200.150	192.168.200.100	TCP	66 41182 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535438 Tscr=4294952466
29 36 .775238694	192.168.200.150	192.168.200.100	TCP	74 55686 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=0 WS=128
30 36 .775238694	192.168.200.150	192.168.200.100	TCP	74 55686 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535438 Tscr=0 WS=128
31 36 .775524294	192.168.200.150	192.168.200.100	TCP	74 53962 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 SACK_PERM Tsva=810535439 Tscr=0 WS=128
32 36 .775589900	192.168.200.150	192.168.200.100	TCP	68 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 36 .775619454	192.168.200.100	192.168.200.150	TCP	68 41394 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 Tscr=4294952466
34 36 .775619454	192.168.200.100	192.168.200.150	TCP	66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 Tscr=4294952466
35 36 .775619454	192.168.200.100	192.168.200.150	TCP	74 88 - 53692 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1468 SACK_PERM Tsva=810535439 Tscr=4294952466
36 36 .775797994	192.168.200.150	192.168.200.100	TCP	74 88 - 53862 [SYN, ACK] Seq=0 Ack=1 Win=5792 Win=0 MSS=1468 SACK_PERM Tsva=4294952466 Tscr=810535439 WS=64
37 36 .775803786	192.168.200.100	192.168.200.150	TCP	66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 Tscr=4294952466 Tscr=810535439 WS=64
38 36 .775813232	192.168.200.100	192.168.200.150	TCP	66 53862 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 Tscr=4294952466
39 36 .775861954	192.168.200.100	192.168.200.150	TCP	66 41182 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 Tscr=4294952466
40 36 .775861954	192.168.200.100	192.168.200.150	TCP	66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 Tscr=4294952466
41 36 .776080353	192.168.200.100	192.168.200.150	TCP	68 53902 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535439 Tscr=4294952466

Figura 3: Raffica iniziale sulle porte principali: evidenza delle porte aperte (Telnet, FTP, HTTP) e chiuse (HTTPS).

2.5 Enumerazione Infrastruttura e Mail (Second Wave)

Proseguendo la scansione (dal pacchetto 42 in poi), l'attaccante sposta il focus dai servizi di accesso remoto ai servizi di infrastruttura e condivisione file. Questa fase evidenzia una chiara distinzione tra i protocolli supportati dalla macchina vittima.

L'analisi del traffico mostra:

- File Sharing (Critico):** Vengono rilevate aperte le porte **139 (NetBIOS-SSN)** e **445 (Microsoft-DS)**. La presenza della porta 445 aperta su un sistema Linux/Unix (come indicato dal banner iniziale) suggerisce la presenza del servizio **Samba**, un vettore di attacco frequente per vulnerabilità di tipo RCE (es. SambaCry).
- Servizi Mail:** È presente una configurazione parziale. La porta **25 (SMTP)** risulta aperta (pacchetto 62), mentre i protocolli di ricezione posta (**POP3 porta 110, IMAP porta 143**) e le varianti sicure (**995, 587**) vengono rifiutati con un RST dalla vittima.
- DNS:** Viene rilevata aperta anche la porta **53 (Domain Name System)**.

Evidenza Tecnica: Le righe 66-68 dello screenshot mostrano nuovamente l'invio dei pacchetti ACK da parte dell'attaccante verso le porte 445, 139, 25 e 53. Questo conferma che anche per i servizi infrastrutturali è stata utilizzata una connessione TCP completa, lasciando tracce evidenti nei log del servizio Samba e del Mail Transfer Agent.

39 36 .//5813292 192.168.200.109 192.168.200.109 TCP 60 520002 - 89 [ACK] Seq=3 ACK=1 Win=0 TSval=810535439 TSecr=0
39 36 .775601664 192.168.200.109 192.168.200.109 TCP 60 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40 36 .775975870 192.168.200.109 192.168.200.109 TCP 60 55656 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41 36 .776058583 192.168.200.109 192.168.200.109 TCP 60 53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42 36 .776179338 192.168.200.109 192.168.200.109 TCP 74 50684 - 199 [SYN] Seq=0 Win=0 TSval=810535439 TSecr=0 WS=128
43 36 .776233303 192.168.200.109 192.168.200.109 TCP 74 50684 - 199 [SYN] Seq=0 Win=0 TSval=810535439 TSecr=0 WS=128
44 36 .776266119 192.168.200.109 192.168.200.109 TCP 74 46448 - 100 [SYN] Seq=0 Win=0 TSval=810535439 TSecr=0 WS=128
45 36 .776385094 192.168.200.109 192.168.200.109 TCP 74 33942 - 445 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
46 36 .776402590 192.168.200.109 192.168.200.109 TCP 74 49814 - 254 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
47 36 .776451284 192.168.200.109 192.168.200.109 TCP 60 199 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 36 .776451357 192.168.200.109 192.168.200.109 TCP 60 995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 36 .776478261 192.168.200.109 192.168.200.109 TCP 74 40099 - 139 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
50 36 .776501664 192.168.200.109 192.168.200.109 TCP 74 40099 - 139 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
51 36 .776512221 192.168.200.109 192.168.200.109 TCP 74 60932 - 123 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
52 36 .776586661 192.168.200.109 192.168.200.109 TCP 74 49654 - 110 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
53 36 .776671271 192.168.200.109 192.168.200.109 TCP 74 37282 - 53 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
54 36 .776720715 192.168.200.109 192.168.200.109 TCP 74 54898 - 589 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
55 36 .776720715 192.168.200.109 192.168.200.109 TCP 60 50003 - 3408 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56 36 .776843423 192.168.200.109 192.168.200.109 TCP 74 41534 - 487 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
57 36 .776994822 192.168.200.109 192.168.200.109 TCP 74 445 - 33942 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=0 WS=64
58 36 .776994942 192.168.200.109 192.168.200.109 TCP 60 256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 36 .776994961 192.168.200.109 192.168.200.109 TCP 74 139 - 46994 [SYN, ACK] Seq=0 Ack=1 Win=0 TSval=810535440 TSecr=0 WS=64
60 36 .776995064 192.168.200.109 192.168.200.109 TCP 60 143 - 46994 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 36 .776995082 192.168.200.109 192.168.200.109 TCP 74 139 - 46994 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62 36 .776995082 192.168.200.109 192.168.200.109 TCP 60 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 36 .776995122 192.168.200.109 192.168.200.109 TCP 74 53 - 37282 [SYN, ACK] Seq=0 Ack=1 Win=0 TSval=810535440 TSecr=0 WS=64
64 36 .776995162 192.168.200.109 192.168.200.109 TCP 60 500 - 54894 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 36 .776995162 192.168.200.109 192.168.200.109 TCP 66 33942 - 53 [ACK] Seq=1 Ack=1 Win=0 TSval=810535440 TSecr=4294952466
66 36 .776995162 192.168.200.109 192.168.200.109 TCP 66 46994 - 53 [ACK] Seq=1 Ack=1 Win=0 TSval=810535440 TSecr=4294952466
67 36 .776995230 192.168.200.109 192.168.200.109 TCP 66 60632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68 36 .776995230 192.168.200.109 192.168.200.109 TCP 66 37282 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69 36 .777118481 192.168.200.109 192.168.200.109 TCP 60 487 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 36 .777143092 192.168.200.109 192.168.200.109 TCP 74 50699 - 162 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
71 36 .777143092 192.168.200.109 192.168.200.109 TCP 74 50699 - 162 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
72 36 .777143092 192.168.200.109 192.168.200.109 TCP 74 50699 - 162 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
73 36 .777337334 192.168.200.109 192.168.200.109 TCP 74 49786 - 78 [SYN] Seq=0 Win=0 TSval=810535440 TSecr=0 WS=128
74 36 .777430632 192.168.200.109 192.168.200.109 TCP 60 707 - 56998 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75 36 .777430741 192.168.200.109 192.168.200.109 TCP 60 436 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 36 .777473921 192.168.200.109 192.168.200.109 TCP 74 36138 - 589 [SYN] Seq=0 Win=0 TSval=810535441 TSecr=0 WS=128
77 36 .777473921 192.168.200.109 192.168.200.109 TCP 74 36138 - 589 [SYN] Seq=0 Win=0 TSval=810535441 TSecr=0 WS=128
78 36 .777523082 192.168.200.109 192.168.200.109 TCP 60 98 - 34128 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36 .777523149 192.168.200.109 192.168.200.109 TCP 60 78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80 36 .777680898 192.168.200.109 192.168.200.109 TCP 74 41874 - 56 [SYN] Seq=0 Win=0 TSval=810535441 TSecr=0 WS=128
81 36 .777680898 192.168.200.109 192.168.200.109 TCP 74 51506 - 439 [SYN] Seq=0 Win=0 TSval=810535441 TSecr=0 WS=128
82 36 .777680898 192.168.200.109 192.168.200.109 TCP 60 98 - 36048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83 36 .77758696 192.168.200.109 192.168.200.109 TCP 60 98 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36 .7777871245 192.168.200.109 192.168.200.109 TCP 60 764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36 .777871293 192.168.200.109 192.168.200.109 TCP 60 435 - 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86 36 .777893290 192.168.200.109 192.168.200.109 TCP 66 33042 - 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87 36 .777912717 192.168.200.109 192.168.200.109 TCP 66 46998 - 138 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88 36 .777985759 192.168.200.109 192.168.200.109 TCP 66 60632 - 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466

Figura 4: Seconda ondata: Rilevamento di Samba (445), NetBIOS (139) e SMTP (25).

2.6 Chiusura Sessioni e Noise Scanning

Immediatamente dopo aver completato l'handshake TCP sulle porte target (fase precedente), l'analisi del traffico evidenzia la fase di "Teardown" (smantellamento) delle connessioni. Nello screenshot , alle righe 86-89, l'attaccante invia pacchetti RST, ACK verso le porte precedentemente confermate aperte:

- Porta 445 (SMB)
- Porta 139 (NetBIOS)
- Porta 25 (SMTP)
- Porta 53 (DNS)

Questa azione conferma la natura automatizzata dell'attacco: il tool apre la connessione solo per verificarne l'esistenza e la chiude immediatamente (circa 10ms dopo l'apertura) per minimizzare l'impiego di risorse, pur lasciando traccia nei log.

2.7 Rilevamento Servizi Legacy Critici (Porta 512)

L'analisi approfondita del traffico ha permesso di isolare un evento di sicurezza ad alta criticità che era passato in secondo piano durante la scansione massiva.

Alle righe 164-166, si osserva il rilevamento della porta TCP 512.

- **Contesto:** La porta 512 (tcp/exec) fa parte della suite di comandi "R" (r-commands) di Unix/Linux. È un servizio di esecuzione remota noto per la sua debolezza intrinseca (spesso basata solo sull'autenticazione dell'indirizzo IP tramite file .rhosts, senza richiesta di password).

Dinamica dell'Handshake (Evidence): Anche in questo caso, la sequenza dei pacchetti conferma la tecnica Connect Scan e l'avvenuto contatto con il servizio:

1. **Packet 164:** La vittima risponde [SYN, ACK] dalla porta 512. Il servizio è attivo e in ascolto.
2. **Packet 165:** L'attaccante invia un [ACK] (evidenziato in bianco/blu nello screen). Questo completa la connessione TCP.
3. **Packet 170:** L'attaccante invia [RST, ACK] per chiudere la connessione.

160 36 .781321950 192.168.200.100 192.168.200.150 TCP 74 55360 - 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535445 TSecr=0 WS=128
161 36 .781356928 192.168.200.100 192.168.200.150 TCP 74 45648 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535445 TSecr=0 WS=128
162 36 .781426319 192.168.200.100 192.168.200.150 TCP 74 53246 - 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535445 TSecr=0 WS=128
163 36 .781487169 192.168.200.150 192.168.200.100 TCP 69 910 - 55368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164 36 .781512468 192.168.200.100 192.168.200.150 TCP 66 45648 - 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535445 TSecr=4294952466
166 36 .781021871 192.168.200.100 192.168.200.150 TCP 69 354 - 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167 36 .781048161 192.168.200.100 192.168.200.150 TCP 74 55186 - 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535445 TSecr=0 WS=128
168 36 .781048161 192.168.200.100 192.168.200.150 TCP 74 33096 - 45960 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535445 TSecr=0 WS=128
169 36 .781048161 192.168.200.100 192.168.200.150 TCP 69 563 - 55368 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535445 TSecr=0 WS=128
170 36 .781988537 192.168.200.100 192.168.200.150 TCP 66 45648 - 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535445 TSecr=4294952466
171 36 .782869902 192.168.200.150 192.168.200.100 TCP 66 663 - 35860 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 36 .782126740 192.168.200.100 192.168.200.150 TCP 74 38210 - 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535445 TSecr=0 WS=128

Figura 5: Discovery della porta critica 512 (exec). Il pacchetto 165 (ACK) conferma l'avvenuta connessione.

2.8 Conferma Vulnerabilità R-Services (Porta 514)

Pochi millisecondi dopo la scoperta della porta 512, l'analisi del traffico evidenzia l'apertura di un ulteriore servizio critico correlato.

Alla riga 267, la vittima risponde positivamente a una richiesta di connessione sulla porta TCP 514.

- **Identificazione Servizio:** La porta 514 TCP è standard per il servizio **shell** (cmd). Insieme alla porta 512 (exec) identificata in precedenza, conferma la presenza attiva della suite "R-Services" (rsh, rlogin, rcp).

Anche in questo frangente, il pacchetto n. 268 (ACK) certifica che la connessione è stata pienamente stabilita prima di essere resettata (pacchetto 273), lasciando traccia dell'intrusione nei log del demone inetd/xinetd.

201 30 .7859027/60 192.168.200.100 192.168.200.150 TCP 74 30542 - 712 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535452 TSecr=0 WS=128
202 36 .7888077029 192.168.200.100 192.168.200.150 TCP 74 51396 - 224 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535452 TSecr=0 WS=128
203 36 .7888077029 192.168.200.100 192.168.200.150 TCP 74 56756 - 224 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535452 TSecr=0 WS=128
205 36 .788805799 192.168.200.150 192.168.200.100 TCP 69 956 - 48350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206 36 .788805939 192.168.200.100 192.168.200.150 TCP 66 773 - 36542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
207 36 .788805946 192.168.200.150 192.168.200.100 TCP 74 514 - 51396 [SYN, ACK] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=4294952467 TSecr=810535452 WS=64
208 36 .788833247 192.168.200.100 192.168.200.150 TCP 66 51396 - 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535452 TSecr=4294952467
209 36 .788945111 192.168.200.150 192.168.200.100 TCP 69 224 - 56758 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
210 36 .789034182 192.168.200.150 192.168.200.100 TCP 66 183 - 48824 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
211 36 .789034182 192.168.200.150 192.168.200.100 TCP 66 361 - 40182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
212 36 .789034182 192.168.200.150 192.168.200.100 TCP 66 51396 - 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535453 TSecr=4294952467
213 36 .789034182 192.168.200.150 192.168.200.100 TCP 66 617 - 36846 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
214 36 .789034182 192.168.200.150 192.168.200.100 TCP 74 36546 - 617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
215 36 .789034182 192.168.200.150 192.168.200.100 TCP 74 36548 - 617 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
216 36 .789032784 192.168.200.150 192.168.200.100 TCP 69 617 - 36846 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
217 36 .789378456 192.168.200.150 192.168.200.100 TCP 74 41728 - 618 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
218 36 .789378456 192.168.200.150 192.168.200.100 TCP 74 41728 - 618 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
219 36 .789378456 192.168.200.150 192.168.200.100 TCP 66 68 - 47720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220 36 .790032784 192.168.200.150 192.168.200.100 TCP 74 37596 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
221 36 .790032784 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
222 36 .790032784 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
223 36 .790032784 192.168.200.150 192.168.200.100 TCP 66 68 - 47720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
224 36 .790032784 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
225 36 .790032784 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
226 36 .790032784 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
227 36 .790032784 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
228 36 .790152359 192.168.200.150 192.168.200.100 TCP 69 62 - 34868 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
229 36 .790152359 192.168.200.150 192.168.200.100 TCP 66 88 - 47720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
230 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
231 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
232 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
233 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
234 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
235 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
236 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
237 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
238 36 .790152359 192.168.200.150 192.168.200.100 TCP 66 68 - 47720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
239 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
240 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
241 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
242 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
243 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
244 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
245 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
246 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
247 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
248 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
249 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
250 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
251 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
252 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
253 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
254 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
255 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
256 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
257 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
258 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
259 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
260 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
261 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
262 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
263 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
264 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
265 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
266 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
267 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
268 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
269 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
270 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
271 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
272 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535453 TSecr=0 WS=128
273 36 .790152359 192.168.200.150 192.168.200.100 TCP 74 37598 - 978 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl

• **Packet 997:** L'attaccante finalizza la connessione con [ACK].

986 36 .825283652 192.168.200.100	192.168.200.150	TCP	74 38016 - 72 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
987 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 42048 - 513 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
988 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 686 - 39848 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
989 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 42048 - 3809 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
991 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 42116 - 422 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
992 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 48434 - 457 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
993 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 40666 - 610 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
994 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 513 - 42048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
995 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 686 - 4019 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
996 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 457 - 48434 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
997 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 42048 - 513 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva=810535489 Tscr=0 WS=128
998 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 610 - 40660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
999 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 56144 - 689 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
1000 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 56144 - 690 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
1001 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 56144 - 691 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
1002 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 34698 - 951 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
1003 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 686 - 56144 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1004 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 267 - 58008 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1005 36 .825283652 192.168.200.150	192.168.200.150	TCP	69 85 - 35678 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1006 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 40538 - 70 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
1007 36 .825283652 192.168.200.150	192.168.200.150	TCP	74 40542 - 28 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128
1008 36 .826516492 192.168.200.150	192.168.200.150	TCP	69 951 - 34688 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1009 36 .826516492 192.168.200.150	192.168.200.150	TCP	69 907 - 46854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1010 36 .826591160 192.168.200.150	192.168.200.150	TCP	74 54134 - 27 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535489 Tscr=0 WS=128

Figura 7: Rilevamento del servizio rlogin (Porta 513), che completa la triade dei servizi R vulnerabili.

Successivamente, il traffico è caratterizzato da quello che in gergo forense viene definito "Scanning Noise": una serie di tentativi verso porte non standard o casuali (es. 148, 806, 221, 206) che rispondono invariabilmente con **RST, ACK** (rifiuto), indicando che nessun servizio è in ascolto su di esse.

Estensione dell'Attacco: È fondamentale notare che questo comportamento persiste per tutta la durata residua del file di cattura. L'attaccante ha continuato sistematicamente a scansionare l'intero range di porte (o un sottoinsieme molto vasto), generando un flusso continuo di risposte [RST, ACK] (visibili come un "muro rosso" in Wireshark) per tutte le restanti porte non attive.

69 36 .7771178481 192.168.200.150	192.168.200.100	TCP	69 487 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 36 .7771178481 192.168.200.100	192.168.200.100	TCP	74 38016 - 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 Tscr=0 WS=128
72 36 .7773032991 192.168.200.100	192.168.200.150	TCP	74 34120 - 513 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535440 Tscr=0 WS=128
73 36 .7773379334 192.168.200.100	192.168.200.150	TCP	74 49780 - 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 Tscr=0 WS=128
74 36 .7774416162 192.168.200.150	192.168.200.100	TCP	69 686 - 56144 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75 36 .7774416162 192.168.200.150	192.168.200.100	TCP	69 436 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 36 .7774416162 192.168.200.150	192.168.200.100	TCP	74 56138 - 589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 Tscr=0 WS=128
76 36 .777522490 192.168.200.100	192.168.200.150	TCP	74 52428 - 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 Tscr=0 WS=128
78 36 .777522490 192.168.200.100	192.168.200.150	TCP	69 98 - 34128 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36 .777522490 192.168.200.100	192.168.200.150	TCP	69 41784 - 164 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 Tscr=0 WS=128
80 36 .777522490 192.168.200.100	192.168.200.150	TCP	74 51590 - 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 Tscr=0 WS=128
82 36 .77758636 192.168.200.150	192.168.200.100	TCP	69 580 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83 36 .77758636 192.168.200.150	192.168.200.100	TCP	69 962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36 .777871245 192.168.200.150	192.168.200.100	TCP	69 764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36 .777871245 192.168.200.150	192.168.200.100	TCP	69 764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86 36 .777871245 192.168.200.150	192.168.200.100	TCP	69 33042 - 445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
87 36 .777912717 192.168.200.100	192.168.200.150	TCP	69 46990 - 139 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
88 36 .777912717 192.168.200.100	192.168.200.150	TCP	69 60632 - 25 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
89 36 .778031292 192.168.200.100	192.168.200.150	TCP	69 37282 - 53 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
90 36 .778179978 192.168.200.100	192.168.200.150	TCP	74 51459 - 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 Tscr=0 WS=128
91 36 .778179978 192.168.200.100	192.168.200.150	TCP	74 51459 - 808 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535441 Tscr=0 WS=128
92 36 .7783937030 192.168.200.100	192.168.200.150	TCP	74 54560 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
93 36 .778385846 192.168.200.150	192.168.200.100	TCP	69 148 - 51459 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94 36 .778385948 192.168.200.150	192.168.200.100	TCP	69 890 - 48484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95 36 .778449494 192.168.200.150	192.168.200.100	TCP	69 221 - 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96 36 .778482791 192.168.200.100	192.168.200.150	TCP	74 42420 - 1087 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
97 36 .778482791 192.168.200.100	192.168.200.150	TCP	74 34464 - 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
98 36 .778482791 192.168.200.100	192.168.200.150	TCP	74 54265 - 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
99 36 .778565364 192.168.200.100	192.168.200.150	TCP	69 88 - 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100 36 .778721898 192.168.200.150	192.168.200.100	TCP	69 286 - 43446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101 36 .778759636 192.168.200.100	192.168.200.150	TCP	74 40318 - 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
102 36 .778781327 192.168.200.100	192.168.200.150	TCP	74 51276 - 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
103 36 .778826294 192.168.200.150	192.168.200.100	TCP	69 131 - 54022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104 36 .778864493 192.168.200.100	192.168.200.150	TCP	74 39566 - 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
105 36 .77893427 192.168.200.100	192.168.200.150	TCP	69 30918 - 51420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106 36 .77893427 192.168.200.150	192.168.200.100	TCP	69 677 - 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107 36 .77893427 192.168.200.150	192.168.200.100	TCP	74 47238 - 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
108 36 .779029219 192.168.200.150	192.168.200.100	TCP	69 856 - 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109 36 .779055243 192.168.200.100	192.168.200.150	TCP	74 56542 - 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
110 36 .779122299 192.168.200.150	192.168.200.100	TCP	69 84 - 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111 36 .779145569 192.168.200.100	192.168.200.150	TCP	74 48133 - 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535442 Tscr=0 WS=128
112 36 .779252884 192.168.200.150	192.168.200.100	TCP	69 681 - 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113 36 .779252884 192.168.200.100	192.168.200.150	TCP	74 40318 - 51420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
114 36 .779390462 192.168.200.100	192.168.200.150	TCP	74 46886 - 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535443 Tscr=0 WS=128
115 36 .779354564 192.168.200.150	192.168.200.100	TCP	69 948 - 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116 36 .779378630 192.168.200.100	192.168.200.150	TCP	74 58264 - 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535443 Tscr=0 WS=128
117 36 .779397023 192.168.200.100	192.168.200.150	TCP	74 51262 - 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva=810535443 Tscr=0 WS=128
118 36 .779695648 192.168.200.100	192.168.200.150	TCP	69 214 - 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 36 .779695750 192.168.200.100	192.168.200.150	TCP	69 106 - 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figura 8: Teardown delle connessioni (RST su porte aperte) e prosecuzione su porte chiuse (Noise).

3 Fase 2: Approfondimento Tecnico (Stealth vs Connect)

Questa sezione dettaglia l'analisi forense che ha permesso di determinare l'esatta tipologia di scansione utilizzata.

3.1 Differenze Teoriche: TCP Connect vs SYN Stealth

Per comprendere l'analisi, è fondamentale distinguere le due modalità principali di scansione TCP:

TCP Connect Scan (-sT)	SYN "Stealth" Scan (-sS)
Esegue il <i>Three-Way Handshake</i> completo.	Esegue un handshake parziale (Half-open).
Flow: SYN → SYN/ACK → ACK → RST	Flow: SYN → SYN/ACK → RST
La connessione viene stabilita a livello Applicativo.	La connessione viene interrotta prima di essere stabilita.
Rilevabilità: Alta. Viene registrata nei log di sistema della vittima.	Rilevabilità: Bassa. Spesso invisibile ai log applicativi standard.

Tabella 1: Confronto tecnico tra le tipologie di scansione.

3.2 Analisi Forense

Analizzando la cattura Wireshark, abbiamo isolato la sequenza di pacchetti relativa alla porta **445 (SMB)**, visibile nello screenshot di prima.

La sequenza osservata è la seguente:

1. **SYN (Attaccante → Vittima):** Richiesta di connessione.
2. **SYN, ACK (Vittima → Attaccante):** Conferma disponibilità della porta.
3. **ACK (Attaccante → Vittima):** *Il punto decisivo.* L'attaccante invia il pacchetto ACK (pacc. n. 66), completando la connessione.
4. **RST, ACK (Attaccante → Vittima):** Solo successivamente (pacc. n. 86) la connessione viene abbattuta.

3.3 Deduzione Investigativa

La presenza del pacchetto **ACK** (terzo step dell'handshake) conferma in modo incontrovertibile che si tratta di una **TCP Connect Scan**. Se fosse stata una scansione Stealth, l'attaccante avrebbe inviato un RST immediatamente dopo aver ricevuto il SYN, ACK, senza mai inviare l'ACK finale.

L'analisi dei pacchetti permette di ricostruire con elevata probabilità le opzioni utilizzate nel tool di scansione (Nmap).

1. **Tecnica (-sT):** La presenza del pacchetto **ACK** inviato dall'attaccante (terzo step dell'handshake) prima del RST conferma l'uso della **TCP Connect Scan**. Se fosse

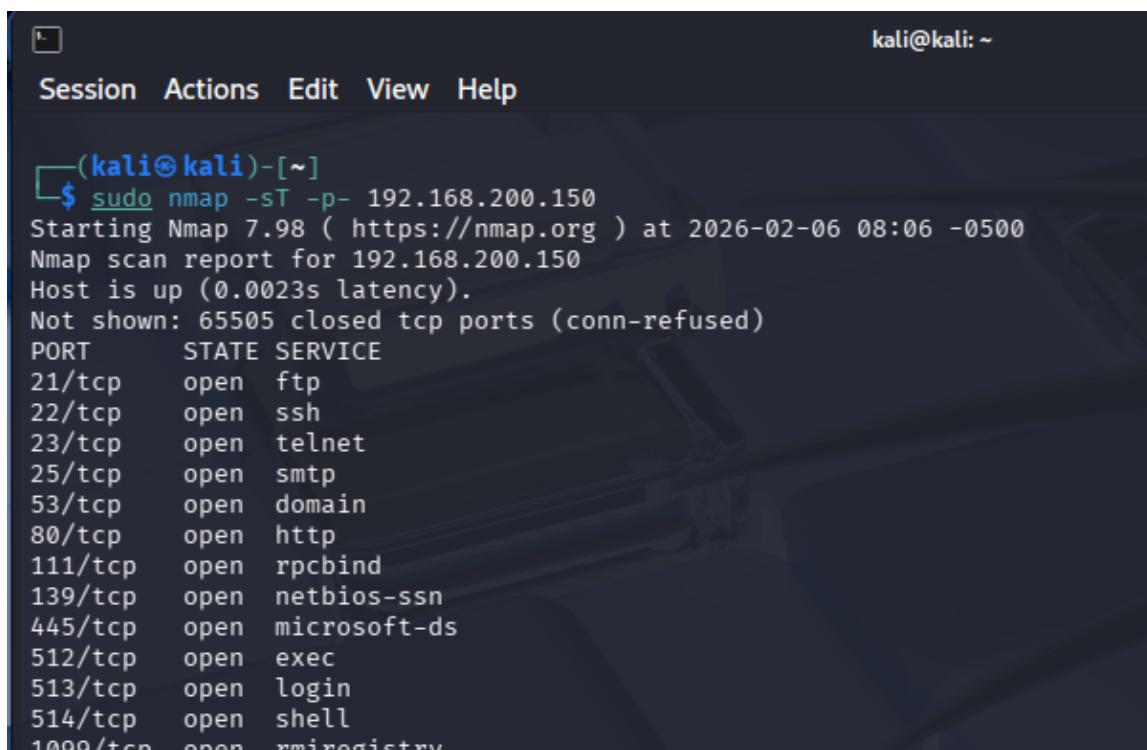
stata una scansione "Stealth" (SYN Scan, default per root), avremmo visto un RST subito dopo il SYN-ACK della vittima.

2. **Estensione (-p-):** L'elevato volume di traffico registrato verso porte non standard e tipicamente chiuse (es. tentativi TCP sulla porta 138, solitamente UDP, o porte randomiche come 118 e 806) indica che l'attaccante non si è limitato alle "Top 1000" porte, ma ha verosimilmente lanciato una scansione sull'intero range di porte (1-65535).
3. **Timing:** La densità temporale dei pacchetti (inviati a intervalli di microsecondi) suggerisce l'uso di un template di timing aggressivo (es. -T4).

Comando Ipotizzato: Sulla base delle evidenze, il comando eseguito dall'attaccante è riconducibile alla seguente sintassi:

```
nmap -sT -p- 192.168.200.150
```

Implicazioni di Sicurezza: L'utilizzo della flag -sT rende l'attacco estremamente "rumoroso". Poiché ogni connessione verso le porte aperte è stata completata a livello di socket, è altamente probabile che i demoni dei servizi (FTP, SSH, Samba) abbiano registrato l'IP dell'attaccante nei log di sistema della vittima (/var/log/auth.log, /var/log/samba/, ecc.), permettendo una facile attribuzione dell'attacco.



The screenshot shows a terminal window with a dark background. At the top, there is a menu bar with options: Session, Actions, Edit, View, Help. On the right side of the menu bar, it says "kali@kali: ~". Below the menu, there is a command prompt area. The user has typed the command: \$ sudo nmap -sT -p- 192.168.200.150. The output of the command is displayed below the command line. It starts with "Starting Nmap 7.98 (https://nmap.org) at 2026-02-06 08:06 -0500" followed by "Nmap scan report for 192.168.200.150". It then states "Host is up (0.0023s latency)". The output continues with "Not shown: 65505 closed tcp ports (conn-refused)" and then lists open ports and services. The list includes: 21/tcp open ftp, 22/tcp open ssh, 23/tcp open telnet, 25/tcp open smtp, 53/tcp open domain, 80/tcp open http, 111/tcp open rpcbind, 139/tcp open netbios-ssn, 445/tcp open microsoft-ds, 512/tcp open exec, 513/tcp open login, 514/tcp open shell, and 1099/tcp open rmiregistry.

```
(kali㉿kali)-[~]
$ sudo nmap -sT -p- 192.168.200.150
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-06 08:06 -0500
Nmap scan report for 192.168.200.150
Host is up (0.0023s latency).

Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
```

Figura 9: Comando probabilmente usato dalla Kali verso la Metasploitable.

4 Fase 3: Risultati dell'Enumerazione

L'attività di scansione ha avuto pieno successo, permettendo all'attaccante di mappare l'intera superficie di attacco. Di seguito sono elencati i servizi confermati come **OPEN**, suddivisi per tipologia e livello di rischio.

4.1 Criticità Massima: Suite "R-Services" (Legacy)

L'analisi ha rilevato l'esposizione della suite completa dei comandi Unix legacy "Berkeley r-commands". Questi servizi sono considerati ad altissimo rischio poiché spesso basano l'autenticazione solo sull'indirizzo IP di provenienza (trust relationship), permettendo accessi root senza password.

- **Porta 512 (TCP exec)**: [Rilevata nel pacchetto 165]. Permette l'esecuzione remota di comandi. È il vettore principale per attacchi RCE immediati.
- **Porta 513 (TCP login)**: [Rilevata nel pacchetto 994]. Servizio *rlogin*, equivalente non cifrato di Telnet/SSH, ma con meccanismi di trust deboli.
- **Porta 514 (TCP shell)**: [Rilevata nel pacchetto 267]. Servizio *rsh* (remote shell). La presenza contemporanea di exec, login e shell conferma che il sistema è obsoleto e non sicuro.

4.2 File Sharing e Infrastruttura

Sono stati identificati servizi che espongono il file system o gestiscono risorse di rete, vettori ideali per l'esfiltrazione di dati o attacchi laterali.

- **Porta 445 (SMB) e 139 (NetBIOS)**: Servizi per la condivisione file Windows/-Samba. Su sistemi Linux datati, la porta 445 è spesso vulnerabile a exploit critici (es. SambaCry o translatable SID).
- **Porta 21 (FTP)**: File Transfer Protocol. Servizio in chiaro, vulnerabile a sniffing delle credenziali e, in alcune versioni (es. vsftpd 2.3.4), contenente backdoor.
- **Porta 111 (RPCbind)**: Mappa i servizi RPC su porte di rete. Utile all'attaccante per enumerare ulteriori servizi (come NFS).
- **Porta 25 (SMTP)**: Mail Server. Configurato per l'invio, ma con le porte di ricezione (POP3/IMAP) chiuse.
- **Porta 53 (DNS)**: Servizio di risoluzione nomi.

4.3 Accesso Remoto e Web

- **Porta 23 (Telnet)**: Accesso amministrativo remoto obsoleto. Tutto il traffico, incluse user e password, viaggia in chiaro.
- **Porta 80 (HTTP)**: Web Server. Potenziale superficie per attacchi web-based (SQL Injection, XSS, CGI vulnerabilities).
- **Porta 22 (SSH)**: L'unico servizio di amministrazione cifrato rilevato, sebbene possa essere soggetto ad attacchi Brute Force.

5 Conclusioni

L'analisi forense ha confermato che l'host 192.168.200.150 è stato oggetto di una **TCP Connect Scan** massiva proveniente dall'IP 192.168.200.100. Poiché l'attaccante ha completato le connessioni TCP (Three-way handshake), l'attività è stata tracciata nei log di sistema della vittima, rendendo l'attacco facilmente attribuibile.

Valutazione del Rischio: **CRITICA** La scansione ha rivelato una compromissione totale della sicurezza perimetrale. I vettori di attacco più gravi identificati sono:

- **Suite R-Services (Porte 512, 513, 514):** Presenza di servizi legacy che permettono l'accesso *root* senza password.
- **File Sharing (Porta 445):** Rischio elevato di esecuzione codice remoto (es. SambaCry).
- **Protocolli in Chiaro (21, 23):** Credenziali esposte a sniffing.

Azioni Richieste: Isolare immediatamente l'host, analizzare i file di log (es. /var/log/auth.log) per confermare eventuali accessi abusivi successivi alla scansione e chiudere le porte non essenziali.